

UNITED STATES DISTRICT COURT

for the
Central District of California

United States of America

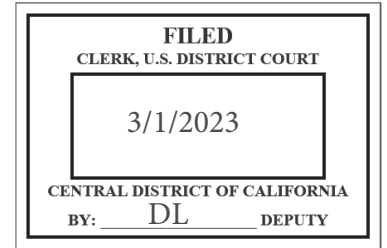
v.

Adrian Corches,

a/k/a Torsten Lund

Defendant

Case No. 2:23-mj-00976-DUTY

**CRIMINAL COMPLAINT BY TELEPHONE
OR OTHER RELIABLE ELECTRONIC MEANS**

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of March 1, 2023 in the county of Los Angeles in the Central District of California, the defendant(s) violated:

Code Section

18 U.S.C. § 1029(a)(2)

Offense Description

Use of unauthorized access devices

This criminal complaint is based on these facts:

Please see attached affidavit.☒ Continued on the attached sheet.

/s/

*Complainant's signature*Jacqueline Cenán, Special Agent,
United States Secret Service*Printed name and title*

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: March 1, 2023 at 11:00 p.m./s/ Rozella A. Oliver*Judge's signature*City and state: Los Angeles, CaliforniaHon. Rozella A. Oliver, United States Magistrate Judge*Printed name and title*

AFFIDAVIT

I, Jacqueline Cenan, being duly sworn, declare and state as follows:

I. PURPOSE OF AFFIDAVIT

1. This affidavit is made in support of a criminal complaint against Adrian Dorin CORCHES, also known as Torsten Lund ("CORCHES"), for a violation of 18 U.S.C. § 1029(a)(2) (use of unauthorized access devices).

2. This affidavit is also made in support of an application for a warrant to search the following digital device in the custody of the United States Secret Service ("USSS"), in Los Angeles, California, as described in Attachment A:

a. Wiko mobile telephone (Gray in color, with a blue phone case) retrieved from CORCHES's person, with unknown model or serial number (the "SUBJECT DEVICE").

3. The requested search warrant seeks authorization to seize evidence, fruits, or instrumentalities of violations of 18 U.S.C. §§ 371 (Conspiracy), 1028 (Fraud and Related Activity in Connection with Identification Documents, Authentication Features, and Information), 1029 (Fraud and Related Activity in Connection with Access Devices), 1344 (Bank Fraud), and 1028A (Aggravated Identity Theft) (collectively, the "Subject Offenses"), as described more fully in Attachment B.

4. Attachments A and B are incorporated herein by reference.

5. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and

information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested complaint and search warrant, and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

II. BACKGROUND OF AFFIANT

6. I am a Special Agent ("SA") with the USSS and have been so employed since March 2021. In this capacity, I am responsible for investigating violations of federal criminal laws relating to financial institution fraud, credit card fraud, bank fraud, cybercrimes, and identity theft. I am a graduate of the Criminal Investigator Training Program conducted at the Federal Law Enforcement Training Center in Glynco, Georgia, as well as the USSS Special Agent Training Course in Beltsville, Maryland. I have received advanced training in financial and cybercrime investigations including the Basic Investigation of Computers and Electronic Crimes Program, Basic Network Intrusion Responder Training, and I have received continued education related to the investigation and prosecution of cybercrimes. I have participated in multiple investigations in connection with fraud and cybercrimes.

III. SUMMARY OF PROBABLE CAUSE

7. Between August 2022 and January 2023, the California Department of Social Services ("DSS") has detected more than

\$38.9 million in stolen funds from victim Electronic Benefit Transfer Cards ("EBT Cards"). Much of this fraud is from two specific programs known as CalFresh and CalWORKs, which help low-income households pay for housing, food, and other necessary expenses. Many of the fraudulent withdrawals are done at specific automated teller machines ("ATMs") in the Central District of California.

8. For example, between on or about January 1, 2023, and on or about January 5, 2023, more than approximately \$117,000 was withdrawn from ATMs at a single financial institution branch located in Toluca Lake, California in Los Angeles County. The unauthorized withdrawals conducted during these five days and at this single bank branch affected approximately 152 victim EBT cardholders. The dates of these withdrawals coincided with the disbursement by DSS of CalFresh and CalWORKs benefits to EBT cardholders.

9. Law enforcement has also reviewed ATM surveillance provided by financial institutions that administer EBT accounts that relate to the fraud scheme at issue. During the unauthorized ATM withdrawals, suspects can often be seen holding stacks of cards and conducting withdrawals from multiple accounts in quick succession at one ATM.

10. On or about March 1, 2023, at approximately 6:00 a.m. PST, law enforcement conducted physical surveillance at a U.S. Bank ATM terminal located at 3461 W. 3rd St, Los Angeles, California 90020 (the "U.S. Bank ATM"), which was identified by DSS as one of the top ATM locations for EBT fraud. At

approximately 6:15 a.m., CORCHES withdrew approximately \$4,970 in cash from the U.S. Bank ATM in rapid succession using approximately four different access devices that were linked to EBT accounts that did not belong to him. Upon detention, CORCHES identified himself to officers as "Torsten Lund." CORCHES was arrested and found to possess: what appeared to be at least four cloned EBT Cards; approximately \$5,608.53 in cash; a false Denmark identification card and Denmark passport, both bearing the alias "Torsten Lund"; and what appear to be two debit cards issued by Bank of America in the name "Torsten Lund." The SUBJECT DEVICE also was seized from CORCHES upon arrest.

IV. STATEMENT OF PROBABLE CAUSE

11. Based on my review of law enforcement reports, conversations with other law enforcement agents, and my own knowledge of the investigation, I am aware of the following:

A. Regulatory Background of CalFresh and CalWORKs Programs

12. DSS is a government agency that administers several benefit and assistance programs for residents of the state of California. One of the assistance programs administered by DSS is called CalFresh (formerly known as food stamps), which helps low-income households purchase food and household items to meet their nutritional needs. Another assistance program administered by DSS is called CalWORKs, which helps low-income families with children pay for housing, food, and other necessary expenses.

13. Residents of California that meet the criteria established by the CalFresh or CalWORKs programs can apply online for benefits at www.getcalfresh.org and www.benefitscal.com. Beneficiaries apply for benefits by submitting their income and number of dependents to determine their benefit eligibility.

14. CalFresh and CalWORKs benefits are issued through EBT Cards. EBT Cards are mailed to an address designated by the account holder and function like traditional debit cards to conduct transactions. For example, you can use an EBT card to make a purchase at a grocery or convenient store by swiping the card at a point-of-sale terminal.

15. The EBT Cards issued under CalFresh and CalWORKs are assigned specific Bank Identification Numbers ("BIN"). A BIN refers to the first five digits of the account number on a debit or credit card and can be used to identify the issuer of the card, like DSS, which administers the CalFresh and CalWORKs programs.

16. Benefits received through the program are typically disbursed to EBT cardholders by DSS during the early days of each month. Those benefits are deposited directly from DSS into the account of the EBT cardholder.

17. The EBT cardholders can then conduct cash withdrawals at ATMs using a personal identification number ("PIN") established by the card holder. The EBT cardholder presents the card at an ATM, inserts the card into the ATM card reader, and

utilizes a PIN to withdraw the funds previously deposited by DSS intended for beneficiaries of the CalFresh or CalWORKs programs.

B. Background on EBT Fraud in the Los Angeles Area and Prior State and Federal Operations

18. Since in or about August 2022, local law enforcement has been working with DSS to investigate a significant increase in unauthorized cash withdrawals utilizing EBT Cards. Based on analysis of victim complaints to DSS, victim complaints to local law enforcement, bank records, and surveillance, law enforcement determined that the majority of the unauthorized cash withdrawals were being conducted with cloned cards.

19. A cloned card can be a blank white plastic card or another debit, credit or gift card that contains altered information on the card's magnetic stripe. Based on my training and experience, I know that suspects will often clone cards by taking stolen card information from a victim card's magnetic stripe and re-encode that stolen information onto another card's magnetic stripe. Cloning these cards allows the suspect to use the card and the DSS benefits added on to the account linked to the card for illicit purchases or unauthorized cash withdrawals.

20. On a legitimate debit or credit card, the information coded on the card's magnetic stripe will match the information embossed on the front of the card. This information includes the account number, expiration date, and cardholder's name, among other information. Whereas on a cloned card, the information coded on the magnetic stripe will not match the information embossed on the front of the card. For example, if

a suspect re-encodes victim EBT card information onto a pre-existing gift card's magnetic stripe or a blank white plastic card with a magnetic stripe, the magnetic stripe will be coded with the EBT card information, but the card itself will still bear the information of the gift card or bear no information if it is a blank white plastic card.

21. Based on my training, experience, and participation in this investigation, I know that the victim card data harvested to clone cards is often obtained from what is colloquially referred to as "skimming activity."

22. The term "skimming" is used to describe activity that involves unlawfully obtaining debit and credit card information by using technological devices to surreptitiously record victim accountholder's debit and credit card numbers and personal identification numbers at, for example, ATMs or point-of-sale terminals. For example, individuals conducting ATM "skimming" may install a skimming device into the card reader of the ATM to record the debit or credit card numbers, as well as a camera or keypad overlay on the ATM keypad to record the associated PIN number. Those individuals will then return to the ATM to collect the card number and PIN information stored on the installed device.

23. As described above, suspects then manufacture cloned and fraudulent debit or credit cards that bear the victim accountholder's account information that was obtained from skimming. Once that information is loaded onto another fraudulent card (e.g., a gift card or blank plastic card),

members of the scheme then use that fraudulent card to withdraw cash from the victim accountholder's bank accounts or to make purchases with the victim accountholder's account.

24. In or about September 2022, local law enforcement conducted a surveillance and arrest operation in the Los Angeles, California area. This operation was planned in response to the large number of unauthorized withdrawals occurring at ATMs in the Los Angeles area during a short period of time. Specifically, law enforcement had analyzed fraudulent EBT withdrawal data and noticed a high volume of unauthorized withdrawals on specific dates and times that coincided with the dates when the majority of benefits are disbursed to EBT cardholders.

25. As a result of this operation, local law enforcement established surveillance at select ATMs that were used to conduct a significant volume of EBT fraud. Law enforcement surveilled those ATMs around the dates when benefits had been disbursed, observed suspects that withdrew a high volume of unauthorized withdrawals and that conducted those withdrawals in rapid succession, and arrested multiple individuals believed to be making fraudulent withdrawals of EBT benefits. As a result, law enforcement arrested approximately 16 suspects. All of the arrested suspects were later determined to be citizens of countries other than the United States who did not have documentation to be lawfully present in the United States. All of the individuals arrested were released from local custody

within hours of their arrest and absconded from any future judicial proceedings.

26. In or about February 2023, in response to a further increase in unauthorized cash withdrawals utilizing EBT Cards after the local law enforcement September 2022 operation, federal law enforcement conducted a similar surveillance and arrest operation in the Los Angeles, California area. Law enforcement established surveillance around the dates when benefits had been disbursed at select high-volume EBT fraud ATMs. Law enforcement arrested three suspects that withdrew a high volume of unauthorized withdrawals and that conducted those withdrawals in rapid succession. Two of those defendants came to the ATM together, possessed 35 cloned EBT Cards at the time of arrest, and later analysis of historic ATM surveillance data showed that they had made more than \$190,000 in past attempted fraudulent EBT withdrawals from a single bank since October 2022. One additional defendant possessed 269 cloned EBT Cards at the time of arrest, and later analysis of historic ATM surveillance data showed that the defendant had made more than \$70,000 in past attempted fraudulent EBT withdrawals from a single bank since January 2023. All three of these defendants were determined to be citizens of Romania, who did not have documentation to be lawfully present in the United States. The three arrested defendants were ordered detained pending trial by the Hon. Karen Stevenson and Hon. Margo A. Rocconi. A federal grand jury returned two indictments against the three defendants for bank fraud, in violation of 18 U.S.C. § 1344; aggravated

identity theft, in violation of 18 U.S.C. § 1028A; use of unauthorized access devices, in violation 18 U.S.C. § 1029(a)(2); and possession of unauthorized access devices, in violation of 18 U.S.C. § 1029(a)(3), in 23-CR-0076-FLA and 23-CR-0077-JFW.

C. Background of Current Operation to Combat EBT Fraud

27. Data provided by DSS, based in part upon reported fraud by victims, reported fraud to local law enforcement, bank records, and surveillance indicates that as of in or about January 2023, there has been approximately \$71.3 million in stolen funds from victim EBT Cards.

28. For the previous six months, between in or about August 2022 and in or about January 2023, in the Central District of California and elsewhere, more than approximately \$38.9 million has been stolen from victim EBT Cards. The majority of these funds were stolen through unauthorized ATM withdrawals.

29. Between on or about January 1, 2023, and on or about January 5, 2023, more than approximately \$7.2 million was stolen from victim EBT Cards largely through unauthorized ATM withdrawals. Of the approximately \$7.2 million stolen from victim EBT Cards in the beginning of January 2023, more than approximately \$2.9 million was stolen, almost entirely through unauthorized ATM withdrawals, in Los Angeles County alone.

30. For example, between on or about January 1, 2023, and on or about January 5, 2023, more than approximately \$117,000 was withdrawn from ATMs at a single financial institution branch

located in Toluca Lake, California in Los Angeles County. The unauthorized withdrawals conducted during these five days and at this single bank branch affected approximately 152 victim EBT cardholders. The dates of these withdrawals coincided with the disbursement by DSS of EBT benefits, including CalFresh and CalWORKs.

31. Based upon my training and experience conducting access device fraud investigations, I know that suspects committing access device fraud schemes will often target particular BINs when harvesting stolen card information collected from skimming devices. Thus, suspects using skimming may target the BIN associated with DSS, in essence, targeting CalFresh and CalWORKs benefits. Moreover, based upon my training and experience, the sheer volume of unauthorized ATM withdrawals occurring during the early days of the month is further indicative that suspects participating in the fraud scheme at issue are targeting EBT Cards because benefits are typically disbursed to EBT cardholders during the early days of each month.

32. Law enforcement has also reviewed ATM surveillance provided by financial institutions that administer EBT accounts that relate to the fraud scheme at issue. During the unauthorized ATM withdrawals, suspects can often be seen holding stacks of cards and conducting withdrawals in quick succession at one ATM. Based upon my training and experience, I know that suspects perpetrating access device fraud schemes will often

conduct unauthorized withdrawals using cloned cards in rapid succession at ATMs.

33. Based upon the rapid succession of unauthorized ATM withdrawals being conducted, the fact that the cards being used to conduct the unauthorized cash withdrawals are nearly all cloned EBT Cards, and the fact that nearly all of the unauthorized withdrawals are happening during the early days of the month, I believe that suspects participating in the fraud scheme at issue are ostensibly targeting EBT Cards.

D. CORCHES Committed EBT Fraud Using Unauthorized Access Devices on March 1, 2023

34. Based upon the large dollar amount being stolen from victim EBT Cards, the number of victims impacted, the concentration of unauthorized ATM withdrawals occurring in particular areas, and the large number of unauthorized ATM withdrawals occurring at singular bank locations, law enforcement conducted a surveillance and arrest operation in March 2023.

35. On or about March 1, 2023, law enforcement was conducting physical surveillance at various bank and ATM locations throughout Los Angeles County, including the U.S. Bank ATM. The U.S. Bank ATM was identified as one of the top ATM locations in Los Angeles for EBT fraud.

36. Based on DSS fraud data, surveillance was conducted on the U.S. Bank ATM on March 1, 2023, beginning at approximately 6:00 a.m.

37. DSS reported to law enforcement that the CalWORKs benefits had been disbursed into recipients' EBT accounts at approximately 12:00 a.m. on March 1, 2023.

38. Based on my training and experience, I know that individuals conducting access device fraud schemes involving EBT often conduct their fraud within hours of CalWORKS benefits disbursement, as they know the funds will be drawn down by the authorized recipients of the EBT account if not first withdrawn by fraud scheme participants.

39. A USSS investigator told me that during this surveillance, law enforcement observed an unknown individual, later identified as CORCHES, arrive on foot and approach the U.S. Bank ATM at approximately 6:13 a.m.

40. A USSS investigator told me that after CORCHES approached the U.S. Bank ATM, law enforcement observed CORCHES, at approximately 6:15 a.m., conduct multiple transactions which appeared to be withdrawals based upon law enforcement observing CORCHES retrieve what appeared to be currency at the conclusion of each transaction. CORCHES appeared to conduct several withdrawal transactions in rapid succession while law enforcement observed for approximately 15 minutes. CORCHES appeared to insert several different cards to conduct withdrawals, and put the retrieved currency and/or cards in his pocket on multiple occasions. Based upon my training and experience, individuals conducting legitimate transactions at ATMs typically conduct a single transaction and do not

transition between multiple payment cards rapidly to conduct several transactions in a short period of time.

41. A USSS investigator told me that while CORCHES was at the U.S. Bank ATM, law enforcement learned from U.S. Bank that the first withdrawal transaction took place on an EBT account associated with a card number ending in 9095 and for a withdrawal amount of approximately \$1,590. At the U.S. Bank ATM, CORCHES then made approximately three additional transactions on EBT accounts associated with card numbers ending in 6236, 8905, and 9168, totaling approximately \$3,380, for an overall loss amount of approximately \$4,970. U.S. Bank also advised law enforcement that CORCHES had unsuccessfully attempted an additional withdrawal transaction totaling \$1,140 from the aforementioned account associated with a card number ending in 9168, for an overall attempted loss amount of \$6,110.

42. A USSS investigator told me that, separately, the U.S. Department of Agriculture ("USDA") - Office of Inspector General ("OIG"), which provides funding for a portion of the EBT program and therefore maintains records associated with EBT cardholders, was able to confirm the full card numbers associated with the cards utilized by CORCHES to conduct the aforementioned ATM transactions. USDA-OIG also confirmed the corresponding cardholder names associated with each card, which consisted of four different California residents - M.G., G.M., E.S. and A.Z. - who were part of the EBT program and who are not CORCHES. In other words, CORCHES was utilizing card numbers belonging to at

least four California residents - the victims - in order to conduct the aforementioned EBT ATM withdrawals.

43. A USSS investigator told me that based on the date and time of the withdrawals hours after CalFRESH benefits disbursement, the identification of the U.S. Bank ATM by DSS as a top ATM location in Los Angeles for EBT fraud, the presence of multiple cards, and his successive ATM withdrawals using multiple EBT card accounts during a short time period, law enforcement detained CORCHES in order to investigate further. When asked to identify himself, CORCHES provided the name "Torsten Lund" and a birth date of September 4, 1972.

44. A USSS investigator told me that law enforcement thereafter arrested CORCHES. CORCHES was read his *Miranda* warning. According to a report from law enforcement present for the arrest, CORCHES did not provide a statement, aside from his alias and date of birth.

45. A USSS investigator told me that law enforcement searched CORCHES and determined he had approximately four cloned cards in his possession. The cloned cards appeared to consist of a variety of prepaid gift cards that had been re-encoded to draw on the EBT accounts described above. At least one of the cloned gift cards also had a number written on it, which, based on my training and experience, likely represents a victim's PIN. Law enforcement also discovered on CORCHES' person what appeared to be two debit cards issued by Bank of America in the name "Torsten Lund," which is a known alias utilized by CORCHES, as described further below.

46. A USSS investigator told me that law enforcement found CORCHES also had approximately \$4,972.53 in cash in his pockets - which was close in value to the approximately \$4,970 in total unauthorized ATM withdrawals - as well as approximately \$636 in cash in his wallet. U.S. Bank ATM surveillance photographs obtained by law enforcement also depicted CORCHES at the U.S. Bank ATM conducting the unauthorized withdrawals using cloned EBT Cards and corroborated law enforcement's surveillance observations.

47. A USSS investigator told me that law enforcement also located on CORCHES' person a purported Denmark identification card bearing the name "Torsten Lund" and birth date of September 4, 1972, as well as a purported Denmark passport bearing the same information. This identification was later confirmed to be fictitious based on fingerprint identification of CORCHES by Immigration and Customs Enforcement ("ICE").

48. A USSS investigator told me that law enforcement subsequently determined CORCHES to be a Romanian national, full name Adrian Dorin Corches, born on April 21, 1972 in Deva, Hunedoara County, Romania, and a holder of a Romanian passport in that name issued on September 16, 2022.

49. A USSS investigator told me that ICE further confirmed that CORCHES had no lawful presence in the United States. Furthermore, a review of historical ICE and Customs and Border Protection records revealed that CORCHES had entered the country illegally via jet ski in October 2022, when he arrived in Marine City, Michigan, from Port Lambton, Ontario, Canada.

50. A USSS investigator told me that USSS subsequently confirmed CORCHES had significant criminal history in Europe for theft-related offenses, including: four year imprisonment for theft in Romania in 2002; imprisonment for unknown duration for theft in Norway in 2005; 19 month imprisonment for aggravated theft in Romania in 2011; and 27 month imprisonment for theft in Finland in 2014.

51. Based on my training and experience, I know that individuals conducting access device fraud schemes will often conceal their true identities by obtaining fictitious IDs to enter the country illegally while evading detection by law enforcement.

52. A USSS investigator told me that the SUBJECT DEVICE was retrieved from CORCHES' pockets following his arrest.

V. TRAINING AND EXPERIENCE REGARDING IDENTITY THEFT CRIMES

53. Based on my training and experience and information obtained from other law enforcement officers who investigate identity theft, I know the following:

a. It is common practice for individuals involved in identity theft, bank fraud, and access device fraud crimes to possess and use multiple digital devices at once. Such digital devices are often used to facilitate, conduct, and track fraudulent transactions and identity theft. Suspects often use digital devices to perpetrate their crimes due to the relative anonymity gained by conducting financial transactions electronically or over the internet. They often employ digital devices for the purposes, among others, of: (1) applying online

for fraudulent credit cards; (2) obtaining or storing personal identification information for the purpose of establishing or modifying fraudulent bank accounts and/or credit card accounts; (3) using fraudulently obtained bank accounts and/or credit card accounts to make purchases, sometimes of further personal information; (4) keeping records of their crimes; (5) researching personal information, such as social security numbers and dates of birth, for potential identity theft victims; and (6) verifying the status of stolen access devices.

b. Oftentimes identity thieves take pictures of items reflecting their stolen identities, including items retrieved from stolen mail or mail matter, with their cellphones.

c. It is also common for identity thieves to keep "profiles" of victims on digital devices. Such "profiles" contain the personal identifying information of victims, such as names, Social Security numbers, dates of birth, driver's license or state identification numbers, alien registration numbers, passport numbers, and employer or taxpayer identification numbers. Identity thieves often keep such information in their cars, storage units, and in their digital devices.

d. It is common for identity thieves, and individuals engaged in bank fraud, access device fraud, and identification document fraud to use equipment and software to print credit and identification cards, to create magnetic strips for credit cards, to use embossing machines to create credit cards, to use laser printers to create checks, and to use

magnetic card readers to read and re-encode credit cards. These types of devices are routinely kept where the person will have easy access to such devices, such as on their person or in their cars or homes or storage units. Software relevant to such schemes can also often be found on digital devices, such as computers.

e. Based on my training and experience, I know that individuals who participate in identity theft, bank fraud, and access device fraud schemes often have co-conspirators, and often maintain telephone numbers, email addresses, and other contact information and communications involving their co-conspirators in order to conduct their business. Oftentimes, they do so on their digital devices. Suspects often use their digital devices to communicate with co-conspirators by phone, text, email, and social media, including sending photos. Suspects may also have paper copies of such records, which they may keep on their person or in their cars, homes, or storage units.

f. Individuals engaged in mail and identity theft often use multiple digital devices, which they may keep on their person or in their cars or homes.

VI. TRAINING AND EXPERIENCE ON DIGITAL DEVICES¹

54. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I

¹ As used herein, the term "digital device" includes the SUBJECT DEVICES as well as any electronic system or device capable of storing or processing data in digital form, including
(footnote cont'd on next page)

know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable

central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as paging devices, mobile telephones, and smart phones; digital cameras; gaming consoles; peripheral input/output devices, such as keyboards, printers, scanners, monitors, and drives; related communications devices, such as modems, routers, cables, and connections; storage media; and security devices.

data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

55. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which

may take substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so many types of digital devices and programs that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

56. The search warrant requests authorization to use the biometric unlock features of a device, based on the following, which I know from my training, experience, and review of publicly available materials:

a. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when

a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

c. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress CORCHES's thumb and/or fingers on the device(s); and (2) hold the device(s) in front of CORCHES's face with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature.

57. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

/ / /
/ / /
/ / /
/ / /
/ / /
/ / /
/ / /
/ / /
/ / /
/ / /
/ / /

VII. CONCLUSION

58. For all of the reasons described above, there is probable cause to believe that CORCHES has committed a violation of 18 U.S.C. § 1029(a)(2) (use of unauthorized access devices). There is also probable cause that the items to be seized described in Attachment B will be found in a search of the SUBJECT DEVICE as described in Attachment A.

Attested to by the applicant in
accordance with the requirements
of Fed. R. Crim. P. 4.1 by
telephone on this 1st day of
March, 2023.

/s/ Rozella A. Oliver
THE HONORABLE ROZELLA A. OLIVER
UNITED STATES MAGISTRATE JUDGE